Practical SOHO Public WLAN Setup

by Cyrus Peikari and Seth Fogie

Since setting up a WLAN can be a bit intimidating for most any small office owner, we included a small 'How To' that explains the risks involved with sharing a WLAN with the public while keeping your business machines secure.

Overview

Wireless networking comes in three main flavors: corporate, small business , and home owner. The amount of money available and the number of expected users/load distinguish these three categories. Thus, the level of support varies greatly. The home user typically needs to ask for a little help, which usually comes in the form of someone's kid or the neighborhood computer expert. Corporations obtain their support from a consultant or paid staff. However, small business owners are in a unique position. Their networks are often a bit too complicated for the local computer geek, but small businesses can't usually afford to keep a hired gun on call, much less a full time staffer. As a result, they are often the victims of poor management and even worse security.

Fortunately, many SOHO vendors realize that this market needs an intelligent device that can simply be installed and left alone. In recent years, firewalls, servers, and more have been created specifically for this market with much success. However, with the introduction of the wireless network, the SOHO has become a new target for hackers. Thanks in part to the popularity of wireless networks and the demand from the traveling customer, small businesses everywhere are starting to share their WLAN's with the general public. Coffee shops, restaurants, hotels, libraries, and more are creating hot spots using their own Internet connection to provide customers with free web access.

While this is good news for users, many of these companies are putting themselves at risk of attack. Since they are sharing the Internet connection with their customers, the wireless users are often able to access both the internal network and the computers connected to them. In other words, using some simple commands, a wireless user can determine the internal addressing of the computers and gain access to their files and services. Since many of these machines are rarely updated, there exists a potentially disastrous situation that is often not realized until too late.

To help fill the gap for this group of businesses, this short section will provide an overview of some options that can help keep a company's machines secure, while allowing wireless access to the general public. Using cheap and common devices we will offer a solution to create a secure network, while maintaining a WLAN.

The Threat

Before taking any step, it is important to understand what you are protecting and what you are protecting against. It is best if you actually take a few minutes and see what you have to lose. Items such as proprietary information, credit card numbers, customer information, and other sensitive data may not seem like much, but in the wrong hands a list of 100,000 credit cards can be quite valuable. This list will help you determine the value of your resources and will provide you with some foundation for a cost-to-risk argument. While security is a very important subject, a small coffee shop that only owns one computer does not need to purchase a $30,000 firewall solution. In fact, if your assets demand that level of security, you should ignore this section; you need a stronger solution.

Typically, there are two main threats that a SOHO owner needs to worry about with regards to a hacker. First is the threat of the accessible file or service. One of the biggest issues many businesses have is their love of file sharing. Often there will be one computer or more that have shares enabled, in which they store all their key database files. Unfortunately, if this computer is on the same network as the WLAN, any wireless user can also access these files.

Related to this are shared services. One of the most commonly abused services is the web server, of which IIS is the most notorious. Since business machines are often not updated, and thus not secured, a hacker with access to the machine could quickly exploit some buffer overflow and gain access to a vulnerable service. In other words, if a business machine was on a network accessible to the WLAN and the machine was running an unpatched IIS, it could be hacked.

The second type of threat is that of sniffing. Although many people consider sniffing to be an abstract issue,, in reality sniffing is one of the most popular and common ways that hackers gain access to computer systems. In fact, since the inception of the wireless network, sniffing has been reborn and has become a popular past time of many hackers. The reason is found in the fact that a wireless sniffer captures everything traveling via the airwaves, and more. Using switching tricks in combination with ARP spoofing attacks, a hacker can capture data that travels over the internal wired network as well. This does depend on the setup of the access point, and where it is located in the network, but if the internal network shares the same IP range as the wireless nodes (i.e. they are on the same network), it is possible to capture data.

In other words, if a wired or wireless user checks their email from a regular POP server, their user name and password will be sent in plain text over the network, and could be captured by a sniffer. Since many people use the same password for everything, a hacker could use this captured information to his/her advantage. In addition, any broadcast packets will go out over the airwaves for all to see. Knowing this, a hacker can learn a lot of valuable information about the inside of a network and what services are running.

One ironic example of this security threat occurs yearly at the famous Defcon security conference. To assist attendees, Defcon offers wireless Internet access during the three day show. Many people use this connection to check their email. Unfortunately for them, at any

one time there are about 50 hackers capturing data, including the user name and password needed to access the email account. To help the victims understand their crime, Defcon has a wall of shame on which people can post captured passwords. Note: The following link may not work forever.

http://www.techfreakz.org/defcon10/?slide=38

The Solution

Now that you have an understanding of what is at risk, let's take a look at a cheap solution that can protect a business's assets yet allow WLAN access. The following is a diagram of a network solution that would enable a business to share a WLAN connection with its own business machines, yet keep some form of security in place. An explanation will follow.

The first step in setting up this network is to purchase the equipment. The following is a list of general equipment pieces. While we do mention a Netgear router, there are many others that work well. However, be careful what you select because some routers do not support VPN throughput, Macs, etc.

- DSL/Cable Modem: Typically provided by the ISP. This could be an actual DSL/Cable modem, or a router depending on the ISP and the level of access required.

- DSL Router/Switch ($50-$100 each): You will need two of these devices. The router should be able to connect to your DSL connection, so be sure it is supported by the ISP. Due to the different types of authentication and variations on network configurations, ISP requirement vary. For example, the BEFW11S4 Linksys DSL router will not work with PPPoA, but will work with PPPoE. In this case, you could use a Netgear 114 series. Whatever choice you make, the router should include a NAT firewall at a minimum, or you can upgrade the firewall to include an Intrusion Detection System and more enhanced firewall protection.

- Wireless Router/Access Point ($100-$200): While a simple access point will get the job done, a wireless router will allow you to define a specific range of IP addresses for your wireless nodes, and thus allow you to have a separate network. This will create a virtual boundary between wireless users and the internal network data, which reduces the possibility of an attacker sniffing the network.

- Patch cables (inexpensive): You will need several patch cables. These can be purchased online or at your local computer shop.

Once you have the equipment, it is time to put it together and set up the IP addresses. This is by far the most important part, and will require you attention. While the equipment will most likely work if you simply plug it in, you will not be secure because every system will be on the same network. Step through the following instructions:

1. Setup and plug in the DSL Modem and DSL Router/Switch #1.

2. Install a network cable running from the DSL modem into the WAN port of the router. This port is usually set apart from the ports used for the built in switch.

3. Configure the DSL Router #1 to connect to your ISP (instruction vary on this and will probably be included with your ISP package).

4. Configure the DSL Router #1 with a LAN IP address of 192.168.0.1/255.255.255.0 and let it act as a DHCP server so it can automatically assign IP addresses to any connected devices. We suggest you use the range of 192.168.0.5-192.168.0.254 for you DHCP. This will allow you to setup your other internal routers with static IP's, as well as a shared printer. A static IP for these devices helps to avoid confusion.

5. Test your network/Internet connection at this point to be sure you successfully configured your router. If there is no connection, troubleshoot as required.

6. Setup and plug in the DSL Router #2.

7. Install a network cable from Port 2 of the DSL Router #1 to the WAN Port on DSL Router #2. Note: Port 1 may be typically used as well; however, some switches use this as the uplink port to allow you to expand your network. You do not need this option and to avoid confusion, we suggest you use port two and three for our illustration.

8. Configure the WAN side of DSL Router #2 to accept a dynamic IP address or specify a static IP address of 192.168.0.2/255.255.255.0. Note, if you use a static IP, ensure the DSL Router #1 was configured as suggested.

9. Set the LAN IP address as 10.0.0.1/255.255.255.0 and configure it as a DHCP server.

10. Plug a business machine into the DSL Router #2 and test your Internet connection. Make sure you have an IP address assigned to the computer by clicking on Start -> Run and typing 'cmd' followed by 'ipconfig' if Windows XP/NT/2000 and 'winipcfg' if Win9x/ME (select Ethernet card adapter). Your network card should have an IP address of 10.0.0.*. If you are using a Mac (OS X) or *nix, you will need to open a shell window and type 'ifconfig'.

11. Setup and plug in the WLAN Router.

12. Install a network cable from port three on the DSL Router #1 to the WAN port on the WLAN Router.

13. Configure the WAN side of the WLAN Router to accept a dynamic IP address or specify a static IP address of 192.168.0.3/255.255.255.0. Again, if you use a static IP, ensure the DSL Router #1 was configured as suggested.

14. Set the LAN IP address as 192.168.1.1/255.255.255.0 and configure it as a DHCP server.

15. Setup a wireless client and test your Internet connection. Make sure you have an IP address assigned to the computer by clicking on Start -> Run and typing 'cmd' followed by 'ipconfig' if Windows XP/NT/2000 and 'winipcfg' if Win9x/ME (select Ethernet card adapter). Your network card should have an IP address of 192.168.1.*. If you are using a Mac (OS X) or *nix, you will need to open a shell window and type 'ifconfig'.

    At this point you should have a working network. You can test your security by using a wireless client and attempting to ping 10.0.0.1. If you get a result, something is wrong. Using this approach, you have used your equipment to setup three separate networks, which will help prevent sniffing. In addition, you have isolated your business machines from the wireless side, which will stop hackers.

    This short write up demonstrates a cheap (< $500) solution that can allow a business machines and the general public to share the same Internet connection. While it is not fool proof, a hacker would have a very difficult time trying to gain access to the business machines. As illustrated, the setup of this network is not difficult or expensive, which means there is no excuse to practice safe networking.